MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

# "AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

# TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

# O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

## MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

**Muassis:** Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
**Chop etish tili:** O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

**Учредитель:** Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
**Язык издания:** узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

**Founder:** Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
**Language of publication:** Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

**2023 yil, Tom 1, №4**
**Vol.1, Iss.4, 2023 y**

**ELEKTRON ILMIY JURNALI** **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz



**FARG’ONA - 2023 YIL**

**Jurnal quyidagi bazalarda indekslanadi:**

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · DRJI Directory of Research Journals Indexing

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

# Криптография на основе эллиптических кривых (ECC)

**Обухов Вадим Анатольевич,**
ассистент кафедры «Информационные технологии»
Ферганского филиала
Ташкентского университета информационных
технологий имени Мухаммада Ал-Хорезми,
e-mail: wendigo_chelsea@mail.ru

Аннотация. Криптография с эллиптической кривой (ECC), как одна из наиболее важных современных криптографий, более надежна, чем большинство других криптографий, как с точки зрения безопасности, так и с точки зрения надежности, поскольку она использует эллиптическую кривую для построения и в то же время использует математические операции для шифрования и генерации ключей. В то же время криптография на основе эллиптических кривых может продолжать улучшать скорость и интенсивность за счет совершенствования ускорителей, скалярного умножения и скорости обработки ордеров.

Ключевые слова: криптография на основе эллиптических кривых (ECC); криптография; код RSA; алгоритм цифровой подписи на основе эллиптических кривых (ECDSA).

**Введение.** Криптография – это искусство тайной передачи информации. Сегодня людям нужна криптография, чтобы побеждать в войнах, строить Интернет и так далее. Криптография является важным инструментом для развития человеческого общества.

В этой статье мы суммировали введение в криптографию, введение в эллиптические кривые, принцип работы ECC, сравнение ECC с другими кодами, прорыв в ECC и применение ECC, используя метод обзора литературы [1].

Был представлен обзор развития ECC. Сравнение может прояснить преимущества и недостатки ECC. Чтобы внести некоторые прямые улучшения, введение в эллиптические кривые и принципы работы ECC может рассказать общественности об ECC; введение в криптографию может повысить осведомленность общественности о криптографии; а применение ECC может помочь людям узнать, как ECC действительно помогает им в повседневной жизни. Прежде всего, эта статья помогает большему количеству людей узнать о криптографии, особенно ECC, и о том, как вместе внести некоторые улучшения в будущее. Кроме того, в этой статье приводятся некоторые практические пути и направления улучшения ECC, давая краткое изложение того, что люди делали для его улучшения раньше.

**Литературный обзор и методология.** Криптография – это искусство сокрытия информации. Люди используют криптографию для передачи информации.

Криптография имеет долгую историю; она была открыта около 400 лет назад. До 1949 года люди использовали классические коды. Классические коды имеют низкую интенсивность, а значит, их легко взломать. Между 1950 и 1975 годами криптография постепенно проникла в сознание людей и стала наукой. С 1976 года по настоящее время ключ в криптографии добился большого прогресса. С этого момента криптография начала делиться на несколько ветвей.

*Классификация криптографии.*

После того, как криптография начала иметь ответвления, криптография была разделена на симметричную и асимметричную криптографию (криптографию с открытым ключом). Среди них криптография с открытым ключом является основным направлением изучения криптографии, а также самой невзламываемой криптографией.

*Криптография с открытым ключом.*

Криптография RSA и криптография на основе эллиптических кривых (ECC) являются двумя основными кодами криптографии с открытым ключом.

Криптография с открытым ключом в основном использует математические вычисления для шифрования и дешифрования. Например, криптография RSA использует огромное число, которое трудно разделить на два больших простых числа, чтобы сделать код более надежным [2].

Криптография с открытым ключом более современна, чем традиционная криптография, и ее безопасность выше, чем у традиционной криптографии, поскольку длина ее ключа больше, а для ее расшифровки требуется больше вычислений. Однако криптография с открытым ключом не заменит полностью традиционную криптографию, поскольку требует большого количества вычислений, поэтому ее можно использовать только для подписей и управления ключами.

| | **Традиционная криптография** | **Криптография с открытым ключом** |
|---|---|---|
| Базовые требования | 1. Отправители и получатели должны использовать общий ключ. | 1. Отправитель владеет одним ключом шифрования или дешифрования, а получатель — другим. |
| | 2.Отправители и получатели должны использовать один и тот же ключ и один и тот же алгоритм. | 2. При шифровании и дешифровании используется один и тот же алгоритм, но разные ключи. |
| Требования безопасности | 1. Не зная ключа, невозможно расшифровать | 1. Не зная ключа, невозможно расшифровать |
| | 2. Если известен только алгоритм и несколько зашифрованных текстов , подтвердить ключ невозможно. | 2. Если известен только один ключ и несколько зашифрованных текстов , невозможно подтвердить другой ключ. |
| | 3.Ключ следует хранить в тайне. | 3. Закрытый ключ должен храниться в тайне. |

***Таблица 1 (Table 1). Сравнение традиционной криптографии и криптографии с открытым ключом.***

*Эллиптические кривые.*

Криптография с эллиптической кривой — важный тип шифрования в криптографии с открытым ключом, который использует эллиптическую кривую для шифрования и дешифрования.

Эллиптическая кривая — это гладкая аффинная кривая с родом 1 в области определения, и ее выражение можно записать как $y^2 = x(x-1)(x-\lambda)$, $\lambda \neq 0,1$, или $y^2 + ay = x^3 + bx^2 + cx + d$. Если характеристики области не 2 и 3, то ее также можно записать как $y^2 = x^3 + ax + b$.

Графики эллиптических кривых изменяются в зависимости от их коэффициентов, как показано на графиках ниже [3].

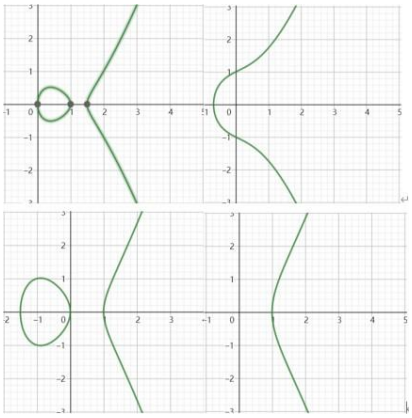


***Рисунок 1 (Picture 1). Четыре разные эллиптические кривые.***

Эллиптические кривые имеют несколько приложений, таких как криптография эллиптических кривых (ECC), алгоритм цифровой подписи эллиптических кривых (ECDSA) и т. д.

Чтобы понять криптографию эллиптических кривых, нам также необходимо знать определение группы.

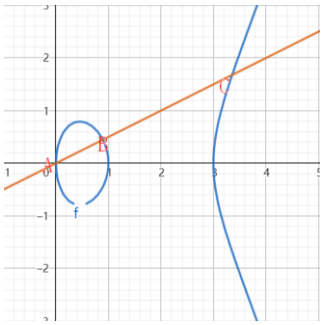
Если непустая группа $G$ определена как имеющая операцию «·», и эта операция выполняется:

1. $\forall x, y \in G$, удовлетворяют значение $x \cdot y \in G$
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
3. $\forall x \in G$, $\exists p$, так, как $p \cdot x = x$
4. $\forall x \in G, \exists y$, так, как $x \cdot y = y \cdot x = q$

тогда мы можем сказать, что $G$ — группа относительно операции «·». Если $G$ также удовлетворяет коммутативной аксиоме, то $G$ - Абелева группа.

*Аддитивная группа на эллиптических кривых.*

На эллиптической кривой нам нужно определить «аддитивную группу» для последующих криптографических вычислений.



$$(P + xA\ ) - кxB$$

***Рисунок 2 (Picture 2). Четыре разные эллиптические кривые.***

На эллиптической кривой мы случайным образом выбираем две точки $A$ и $B$. Затем проводим линию $AB$ и пересекаем эллиптическую кривую в точке $C$. Затем определяем $A+B+C$.

Если $A$ и $B$ — одни и те же точки, то $C$ — точка пересечения касательной линии $A$ и эллиптической кривой [4].

Доказано, что аддитивная группа эллиптической кривой соответствует четырем требованиям группы, поэтому она является группой, а также соответствует коммутативной аксиоме, поэтому она является абелевой группой.

*Порядок эллиптических кривых.*

Порядок эллиптической кривой также является важным базовым знанием эллиптической кривой.

Если эллиптическая кривая существует в конечных полях, порядок существует. Порядок — это количество точек в ограниченной области эллиптической кривой.

Основной принцип криптографии с эллиптическими кривыми (ECC).

*Составляющая криптографии с эллиптическими кривыми (ECC).*

Кодовая система состоит из открытого текста, ключа и зашифрованного текста, причем ключ может быть открытым, закрытым или частично открытым и частично закрытым.

*Формирование ключа криптографии с эллиптическими кривыми (ECC).*

Автор случайным образом выбирает две точки $A$ и $B$ на эллиптической кривой, $B$ является кардинальной точкой эллиптической кривой, а $A$ удовлетворяет условию $A = kB$. Затем задаётся для закрытого ключа значение $k$, а для открытого ключа — $A$. Используя аддитивную группу на эллиптической кривой, если мы знаем только $k$ и $B$, легко найти $A$, но если мы знаем только $A$ и $B$, трудно найти $k$ [5].

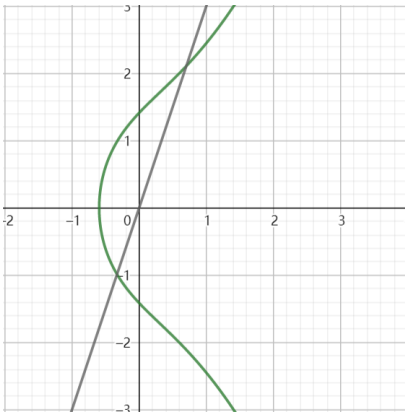


***Рисунок 3 (Picture 3). Линия, проходящая через эллиптическую кривую.***

*Шифрование криптографии с эллиптическими кривыми (ECC).*

Во-первых, кодировщик должен посредством некоторых изменений преобразовать предложения в открытом тексте в несколько чисел.

Затем кодер должен случайным образом найти конкретную эллиптическую кривую.

Установите открытый текст как $P$, выберите число $x$ ($x < n$, $n$ — порядок конкретной эллиптической кривой) случайным образом. Посредством преобразования $Q = (xB, P + xA)$ кодер преобразует открытый текст $P$ в зашифрованный текст $Q$. Сложение в этом преобразовании является обычным алгебраическим сложением. Затем

измените зашифрованный текст $Q$ на слова, внося некоторые изменения [6].

*Расшифровка криптографии с эллиптическими кривыми.*

Декодер получит закрытый ключ $k$, поэтому декодер может использовать уравнение для поиска открытого текста $P$, потому что $(P + xA) - kxB = P + kxB - kxB = P$.

*Причина, по которой ECC использует эллиптические кривые.*

1) Линия, проходящая через случайную точку эллиптической кривой, скорее всего, будет иметь три точки пересечения со всей эллиптической кривой. Это удовлетворяет требованиям добавки к эллиптическим кривым, которые требует ECC.
2) Существует несколько форм эллиптических кривых. Изменение коэффициента может привести к изменению формы всей эллиптической кривой.

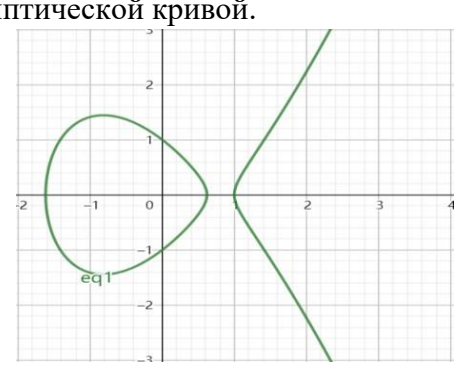



***Рисунок 4 (Picture 4).*** $y^2 = x^3 - 2x + 1$

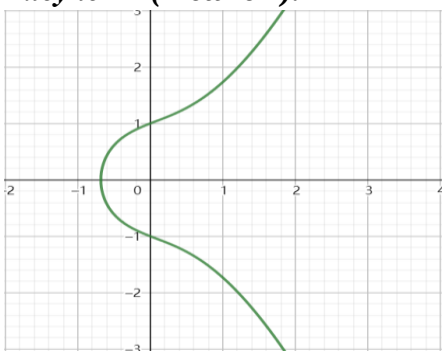


***Рисунок 5 (Picture 5).*** $y^2 = x^3 + x + 1$.

Это удовлетворяет требованию разнообразия эллиптических кривых в ECC.

Сравнение криптографии ECC и RSA

*Сравнение ключевых моментов криптографии ECC и RSA.*

Ключом к криптографии RSA является то, что большое число, умноженное на два больших простых числа, является открытым ключом и его трудно разобрать. Однако эффективность генерации двух огромных простых чисел ниже, чем у криптографии на эллиптических кривых [7].

Криптография с эллиптической кривой (ECC) использует обратную операцию сложения эллиптической кривой в качестве ключа и позволяет добиться высокого уровня шифрования без сложных операций, поэтому ее эффективность относительно выше. Кроме того, до сих пор не было обнаружено каких-либо очевидных уязвимостей ECC, поэтому это относительно надежная современная криптография.

*Анализ преимуществ криптографии на основе эллиптических кривых (ECC).*

Во-первых, криптография на основе эллиптических кривых имеет более высокий уровень безопасности. Система шифрования с эллиптической кривой обеспечивает более надежную защиту и лучше, чем любой другой алгоритм шифрования, предотвращает атаки, делает веб-сайты и инфраструктуру более безопасными, чем традиционные методы шифрования, что позволяет ECC обеспечить лучшую гарантию безопасности мобильного Интернета [8].

Во-вторых, криптография на основе эллиптических кривых лучше подходит для мобильного Интернета. Криптография с эллиптической кривой имеет относительно короткий ключ длиной 256 бит, поэтому она занимает меньше места для хранения. Поскольку все больше и больше пользователей используют мобильные устройства для выполнения различных действий в Интернете, криптография на основе эллиптических кривых обеспечивает лучшее качество обслуживания клиентов в области безопасности мобильного Интернета.

В-третьих, криптография на основе эллиптических кривых имеет лучшие свойства. Криптография на основе эллиптических кривых

может обеспечить лучшую безопасность при более коротких длинах ключей. Например, стойкость ключа 256-битной криптографии с эллиптической кривой примерно такая же, как и стойкость 3072-битного ключа RSA (в настоящее время нормальная длина ключа RSA составляет 2048 бит). Согласно тестам соответствующих зарубежных органов, время отклика веб-сервера более чем в десять раз быстрее, чем у RSA при использовании алгоритма ECC на серверах Apache и IIS.

*Анализ недостатков криптографии на основе эллиптических кривых (ECC).*

Основным недостатком криптографии на основе эллиптических кривых является ее низкая эффективность. Эллиптическая криптография опирается на математические вычисления для шифрования и дешифрования, а ее надежность зависит от сложности вычислений. Поэтому его расчет огромен, что приводит к низкой эффективности передачи, шифрования и дешифрования [9].

**Результаты.**

*Улучшения Ускорителя.*

Одним из основных недостатков криптографии с открытым ключом является то, что она требует слишком много вычислений и потребляет слишком много энергии и времени, поэтому улучшение ускорителя крайне необходимо для повышения эффективности шифрования и дешифрования эллиптических кривых, а также генерации ключей. Нынешние отечественные и зарубежные студенты университетов, имеющие большой опыт в криптографии на эллиптических кривых, стремятся исследовать способы повышения эффективности и постепенно находят более подходящий ускоритель для криптографии на эллиптических кривых. Например, метод ASIC можно использовать для проектирования и реализации аппаратных ускорителей.

*Ускорение алгоритма скалярного умножения.*

Скорость алгоритма скалярного умножения очень важна для шифрования эллиптической криптографии. Есть два фактора, которые ускоряют алгоритм скалярного умножения: координатное представление и представление цепочки экспоненциального сложения. Представление обратных координат позволяет избежать обратной операции в конечной области. Цепочка экспоненциального сложения может обеспечить скалярное умножение с как можно меньшим количеством групп эллиптических кривых.

В настоящее время самым современным стандартом является координатное представление: нечетные объекты используют координаты Якоби, а четные — координаты LD. Повышенная скорость алгоритма скалярного умножения может с замечательным эффектом применяться к популярному оборудованию.

*Улучшения порядка расчета.*

Используя метод комплексного умножения, можно легко найти эллиптическую кривую, но для дальнейшего усиления безопасности системы паролей в криптографии эллиптическая кривая имеет тенденцию генерироваться случайным образом. Но эллиптические кривые, необходимые для криптографии эллиптических кривых, должны иметь один и тот же порядок, поэтому поляризация порядка становится важным эффектом при создании эллиптических кривых.

В 1984 году Шуф с помощью алгоритма с полиномиальным временем предложил вычислить порядок метода эллиптических кривых, но фактическая производительность алгоритма очень низкая, поэтому автор не может получить практического применения в криптографии на эллиптических кривых. Затем Элки выдвинул простые числа Элки и простые числа Аткинса, которые в конечном поле имеют более широкий контекст, предложен алгоритм и значительно повышает эффективность расчета порядка эллиптических кривых. Точно так же Лесье предложил метод использования формы способа расчета эффекта, который дал аналогичные результаты. Затем Сато и Харли предложили более

эффективный алгоритм, а также предложили такой же простой и эффективный метод расчета, позволяющий вычислить более выдающийся эффект. На данный момент эта проблема решена почти идеально несколькими криптографами и математиками [10].

*Алгоритм цифровой подписи на основе эллиптических кривых (ECDSA).*

Цифровая подпись не относится к реальной подписи, но закрытый ключ «подписывает» определенную информацию. Другие люди (включая пользователя *Б*) могут проверить, что информация действительно подписана пользователем *А* с помощью открытого ключа пользователя *А*, поскольку информация может быть подписана только закрытым ключом пользователя *А*. Однако цифровые подписи могут использоваться для реальных подписей.

Оператор будет использовать хэш-функцию, которая находится на уровне безопасности, для преобразования открытого текста подписи *P* в зашифрованный текст *Q*. Затем оператор случайным образом генерирует другое число *k (0 < k < n), n* - это порядок циклической подгруппы. *A = kB*, определение *A, B, k* такое же, как и приведенное выше. Затем определяется $X_p$ как координата *X* точки *P*, $r = x_p \bmod n$, $s = (z + rd_A)/k \bmod n$. (*r, s*) — это информация о подписи.

*Алгоритм SM2.*

SM2 имеет преимущества перед RSA с точки зрения безопасности и свойств. Таким образом, SM2 может заменить RSA. Алгоритм SM2 имеет множество применений, например, усиление информационной безопасности.

Существует связь между алгоритмом SM2 и криптографией эллиптических кривых (ECC). Алгоритм SM2 определяет свою кривую путем определения in. Кроме того, чтобы сопоставить кривые с алгоритмами шифрования, в стандарте SM2 идентифицируются другие параметры для использования алгоритмическими программами [11].

**Заключение.** Прежде всего, криптография быстро развивалась с древних времен. Переход от классической криптографии к современной криптографии произошел благодаря эллиптической кривой. Во-вторых, она более надёжна, чем большинство других криптографий, как с точки зрения безопасности, так и с точки зрения надежности, поскольку для построения она использует эллиптические кривые и в то же время использует математические операции для шифрования и генерации ключей.

Во-вторых, криптография на основе эллиптических кривых может продолжать улучшать скорость и интенсивность за счет улучшения ускорителей, скалярного умножения и скорости обработки ордеров.

Наконец, применение эллиптической кривой в цифровой подписи в Интернете и SM2 очень эффективно, что еще раз иллюстрирует важность криптографии с эллиптической кривой.

**Список литературы** (References)**:**

1. Бессалов, А. В. (2017). Эллиптические кривые в форме Эдвардса и криптография.
2. Болотов, А. А., Гашков, С. Б., Фролов, А. Б., & Часовских, А. А. (2006). Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. Изд, 2.
3. Бессалов, А. В., Дихтенко, А. А., & Третьяков, Д. Б. (2011). Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, (4), 33-36.
4. Долгов, В. И. (2008). Эллиптические кривые в криптографии. Системи обробки інформації, (6), 2-10.
5. Жданов, О. Н., & Чалкин, В. А. (2013). Эллиптические кривые: Основы теории и криптографические приложения. М.: Книжный дом «ЛИБРОКОМ», 2013. 200 с.
6. Левин, В. Ю. (2007). Кодирование алфавитов точками эллиптических кривых. Интеллектуальные системы, 11(1-4), 171-184.
7. Марчук, К. С., & Асмыкович, И. (2019). Алгоритм создания электронной подписи на основе групп точек на эллиптической кривой. In МОЛОДЕЖЬ И

НАУКА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ. (pp. 370-373).

8. Обухов, В., Эльнур, Х., & Набижонов, Р. (2023). ПОЭТАПНОЕ ВНЕДРЕНИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН. Research and implementation.
9. Обухов, В., Ходжиматов, Ж., & Набижонов, Р. (2023). РАЗВИТИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В УЗБЕКИСТАНЕ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ. Research and implementation.
10. Обухов, В. А. (2023). Цифровая безопасность данных в блокчейн-сетях. PEDAGOG, 6(10), 304-308.
11. Обухов, В. А., & Хакимов, А. А. (2022). ОСНОВЫ ИСПОЛЬЗОВАНИЯ РЕКУРСИВНЫХ ФУНКЦИЙ В СТРУКТУРАХ ДАННЫХ. Journal of new century innovations, 11(1), 92-99.